zentera™

Securing Chip Collaboration

Reducing Execution Risk; Accelerating the Entire Product Lifecycle

Secure Multiparty Collaboration

Virtual Chamber

Core Features

- Zero Trust, identity-based access controls
- Universal ZTNA
- Overlays Existing Applications/Data
- Role-based access supporting MFA
- On-Prem, In Cloud, or In 3rd Party Networks

Trusted By High-Tech Companies Worldwide

cadence SIEMENS DELTA Ambarella

"Strong protection... easy to use and administer."

Sreeni Kancharla
VP and CISO, Cadence Design Systems

Agent Support

Windows XP and up
Windows Server 2003 and up
Linux kernel 2.6.32 and up (Redhat 5+)
MacOS

Supports Compliance For

ITAR, CMMC v2, NIST SP800-207, NIST SP800-218

Semiconductor Success Requires Everyone Rowing In The Same Direction

Delivering a world-class semiconductor product requires contributions of expertise from dozens of parties, from IP providers and EDA and fab partners to packaging and test facilities. Semiconductor companies manage this web without putting confidential information at risk.

Semiconductor IT and security teams have developed practices for storing sensitive information in physical *chambers*, a group of servers that are walled off from the rest of the network. But physical chambers can take 6-12 months to build, which is why they are reserved for the most sensitive IP – once qualified, they are infrequently updated.

This is also why they aren't more commonly used to support business initiatives - even though a failed tape-out can cost over $10M, delay market entry for 3-6 months, and trigger delays that ripple across the entire ecosystem.

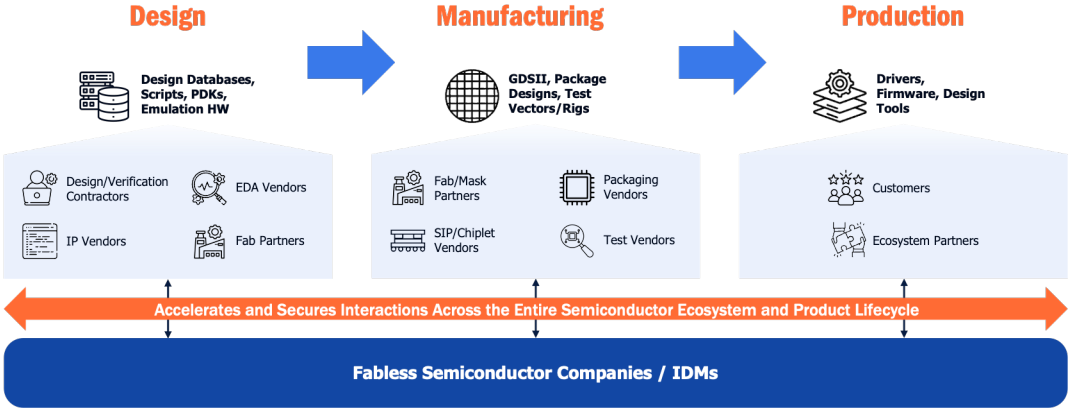
Cut Deployment Time From 6 Months to 6 Hours With Virtual Chambers

A Virtual Chamber shares many of the same benefits – powerful security and access controls to protect assets. However, a Virtual Chamber is software-defined and is far easier to deploy and configure than a physical chamber. This has several key benefits:

- Virtual Chambers can be set up and torn down quickly, making it possible to apply the chamber concept to a much **wider range of use cases** than ever before
- Virtual Chambers can be defined around existing application servers and data, **eliminating the need to transfer data** to a different physical environment
- Virtual Chambers can be **created anywhere** – on-prem, in the cloud, or even inside 3rd party-owned networks

Zentera's Virtual Chambers are natively integrated with Zero Trust Network Access (ZTNA), making it possible to secure 3rd party access even when using unmanaged devices.

Applications Throughout The Semiconductor Lifecycle



Design

- Collaborate directly with IP and EDA vendors to speed up debug and de-risk tapeouts
- Secure chip designs, PDKs, and source code against data leaks
- Secure unmanaged 3rd party contractor access
- Drive interactive design reviews with fab partners
- Enable acquired teams to access design environments on Day 1

Manufacturing

- Collaborate with packaging and system-in-package vendors
- Debug post-silicon issues with fab partners without exposing design files
- Secure and access proprietary and custom test equipment co-located at test houses

Production

- Remotely debug software with GDB without exposing source code or putting customer IP at risk
- Provide trusted ecosystem partners with remote access to company labs

Getting Started

Getting started with Zentera is simple – our orchestrator deploys as a virtual appliance in your network or in the cloud. Once set up, it's easy to install agent software on a server to create a Virtual Chamber and configure user access. Contact sales to learn more or schedule a 15-minute demo to experience how it works.